United Nations A/CN.9/974

General Assembly

: General
ıly 2018

Original: English

United Nations Commission on International Trade Law
Fifty-second session
Vienna, 8–26 July 2019

Draft notes on the main issues of cloud computing contracts

Note by the Secretariat

1. At its fifty-first session, in 2018, the Commission considered the recommendation of Working Group IV (Electronic Commerce) that the Commission should review the draft notes on the main issues of cloud computing contracts at its fifty-second session, in 2019, and authorize its publication or issuance in the form of an online reference tool, in both cases as a work product of the Secretariat (A/CN.9/936, para. 44). After discussion, the Commission decided to review the draft notes on the main issues of cloud computing contracts at its fifty-second session, in 2019.[1]

2. Also at the fifty-first session, the Commission requested the Secretariat to prepare, within existing resources, a pilot online tool containing the draft notes on the main issues of cloud computing contracts, for consideration at its fifty-second session, in 2019. The Commission also requested the Secretariat to prepare a note illustrating the considerations relating to the preparation of the pilot online tool, including budgetary and other implications, and departure from the existing UNCITRAL publication policy.[2]

3. The annex to the present note sets out the text of the draft notes on the main issues of cloud computing contracts, prepared by the UNCITRAL secretariat. The terms appearing in bold are described in the glossary at the end of the draft notes. A note by the Secretariat on a pilot online tool containing the draft notes on the main issues of cloud computing contracts is to be submitted separately in document A/CN.9/975.

[1] *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 150.

[2] Ibid., para. 155.

V.18-05197 (E) 091018 101018

Please recycle

Annex

Notes on the Main Issues of Cloud Computing Contracts (prepared by the secretariat of the United Nations Commission on International Trade Law, 2019)

Contents

		Page
Introduction		5
Part One. Main pre-contractual aspects		6
A.	Verification of mandatory law and other requirements	6
	Data localization	6
	Choice of a contracting party	6
B.	Pre-contractual risk assessment	6
	Verification of information about a specific cloud computing service and a selected contracting party	7
	IP infringement risks	7
	Risks to data security, integrity, confidentiality and privacy	8
	Penetration tests, audits and site visits	8
	Lock-in risks	8
	Business continuity risks	9
	Exit strategies	9
C.	Other pre-contractual issues	9
	Disclosure of information	9
	Confidentiality	9
	Migration to the cloud	10
Part Two. Drafting a contract		11
A.	General considerations	11
	Freedom of contract	11
	Contract formation	11
	Contract form	11
	Definitions and terminology	12
	Minimum contract content	12
B.	Identification of contracting parties	12
C.	Defining the scope and the object of the contract	12
	Service level agreement	12
	Performance measurement	13
	Acceptable use policy	13
	Security policy	14
	Data integrity	14
	Confidentiality clause	14
	Data protection/privacy policy or data processing agreement	15

	Obligations arising from data breaches and other security incidents	16
	Data localization requirements	16
D.	Rights to customer data and other content	17
	Provider rights to customer data for the provision of services	17
	Provider use of customer data for other purposes	17
	Provider use of customer name, logo and trademark	18
	Provider actions as regards customer data upon State orders or for regulatory compliance	18
	Rights to cloud service-derived data	18
	IP rights protection clause	18
	Interoperability and portability	18
	Data retrieval for legal purposes	19
	Data deletion	19
E.	Audits and monitoring	19
	Monitoring activities	19
	Audit and security tests	20
F.	Payment terms	20
	Pay-as-you-go	20
	Licensing fees	20
	Additional costs	21
	Other payment terms	21
G.	Changes in services	21
	Changes in price	21
	Upgrades	21
	Degradation or discontinuation of services	22
	Notification of changes	22
H.	Suspension of services	22
I.	Subcontractors, sub-providers and outsourcing	23
	Identification of the subcontracting chain	23
	Changes in the subcontracting chain	23
	Alignment of contract terms with linked contracts	23
	Liability of subcontractors, sub-providers and other third parties	24
J.	Liability	24
	Statutory limitations to contractual freedom	24
	Other considerations for drafting liability clauses	25
	Provider's standard terms	25
	Possible variations of standard terms	25
	Liability insurance	25
K.	Remedies for breach of the contract	26
	Types of remedies	26

Suspension or termination of services ... 26
Service credits ... 26
Formalities to be followed in case of the breach of the contract ... 26
L. Term and termination of the contract ... 27
Effective start date of the contract ... 27
Duration of the contract ... 27
Earlier termination ... 27
Termination of the contract for convenience ... 27
Termination for breach ... 27
Termination due to unacceptable modifications of the contract ... 28
Termination in case of insolvency ... 28
Termination in case of change of control ... 28
Inactive account clause ... 29
M. End-of-service commitments ... 29
Time frame for export ... 29
Customer access to the content subject to export ... 29
Export assistance by the provider ... 29
Data deletion ... 29
Post-contract retention of data ... 30
Post-contract confidentiality clause ... 30
Post-contract audits ... 30
Leftover account balance ... 30
N. Dispute resolution ... 30
Methods of dispute settlement ... 30
Arbitral proceedings ... 30
Online dispute resolution ... 31
Judicial proceedings ... 31
Retention of data ... 31
Limitation period for complaints ... 31
O. Choice of law and choice of forum clauses ... 31
Considerations involved in choosing the applicable law and forum ... 32
Mandatory law and forum ... 32
Provider or customer home law and forum ... 32
Multiple options ... 32
No choice of law or forum ... 32
P. Notifications ... 33
Q. Miscellaneous clauses ... 33
R. Amendment of the contract ... 33
Glossary ... 34

Introduction

1. The present Notes address the main issues of cloud computing contracts between business entities where one party (the provider) provides to the other party (the customer) one or more **cloud computing services** for the end use. Contracts for resale or other forms of further distribution of **cloud computing services** are excluded from the scope of the Notes. Also excluded from the scope of the Notes are contracts with **cloud computing service partners** and other third parties that may be involved in the provision of the cloud computing services to the customer (e.g., contracts with subcontractors and Internet service providers).

2. Cloud computing contracts may be qualified under the applicable law as a service, rental, outsourcing, licensing, mixed or other type of contract. Statutory requirements as regards its form and content may vary accordingly. In some jurisdictions, parties themselves in their contract may qualify the contract as a contract of a particular type if legislation is silent or vague on that issue; the court would take such qualification into account in interpreting the terms of the contract unless this would contradict the law, court practice, the actual intention of the parties, the factual situation or business customs or practices.

3. The issues addressed in these Notes may arise from cloud computing contracts regardless of the type of **cloud computing services** (e.g., **infrastructure as a service (IaaS)**, **platform as a service (PaaS)** or **software as a service (SaaS)**), their **deployment model** (e.g., **public, community**, **private** or **hybrid)** and payment terms (with or without remuneration). The primary focus of the Notes is on contracts for the provision of public **SaaS**-type cloud computing services for remuneration.

4. The ability to negotiate cloud computing contract clauses would depend on many factors, in particular on whether the contract involves **standardized commoditized multi-subscriber cloud solutions** or an individual tailor-made solution, whether a choice of competing offers exists, and on the bargaining positions of the potential parties. The ability to negotiate the terms of a contract, in particular clauses on unilateral suspension, termination or modification of the contract by the provider and liability clauses, may be an important factor in choosing the provider where the choice exists. Although prepared primarily for parties negotiating a cloud computing contract, the Notes may also be useful for customers reviewing standard terms offered by providers to determine whether those terms sufficiently address the customer's needs.

5. The Notes should not be regarded as an exhaustive source of information on drafting cloud computing contracts or as a substitute for obtaining any legal and technical advice and services of professional advisers. The Notes suggest issues for consideration by potential parties before and during contract drafting without intending to convey that all of those issues must always be considered. The various solutions discussed in the Notes will not govern the relationship between the parties unless they expressly agree upon such solutions, or unless the solutions result from provisions of the applicable law. Headings and subheadings used in the Notes and their sequence are not to be regarded as mandatory or as suggesting any preferred structure or style for a cloud computing contract. The form, content, style and structure of cloud computing contracts may vary significantly, reflecting various legal traditions, drafting styles, legal requirements and parties' needs and preferences.

6. The Notes are not intended to express the position of the United Nations Commission on International Trade Law (UNCITRAL) or its secretariat on the desirability of concluding cloud computing contracts.

7. The Notes consist of two parts and a glossary: part one addresses the main pre-contractual aspects that potential parties may wish to consider before entering into a cloud computing contract; part two addresses the main contractual issues that negotiating parties may face while drafting a cloud computing contract; and the glossary describes some technical terms used in the checklist, to facilitate understanding.

Part One. Main pre-contractual aspects

A. Verification of mandatory law and other requirements

8. The legal framework applicable to the customer, the provider or both may impose conditions for entering into a cloud computing contract. Such conditions may also stem from contractual commitments, including **intellectual property (IP) licences**. The parties should in particular be aware of laws and regulations related to **personal data**, cybersecurity, export control, customs, tax, trade secrets, IP-specific and **sector-specific regulation** that may be applicable to them and their future contract. Negative consequences of non-compliance with mandatory requirements may be significant, including invalidity or unenforceability of a contract or part thereof, administrative fines and criminal liability.

9. Conditions for entering into a cloud computing contract may vary by sector and jurisdiction. They may include requirements to take special measures for the protection of **data subjects' rights**, to deploy a particular model (e.g., **private cloud** as opposed to **public cloud**), to encrypt data placed in the cloud and to register with State authorities a transaction or a software used in the processing of **personal data**. They may also include **data localization** requirements, as well as requirements regarding the provider.

Data localization

10. **Data localization requirements** may arise in particular from the law applicable to personal **data**, accounting data and public sector data and export control laws and regulations that may restrict the transfer of certain information or software to or from particular countries or a region. Compliance with data localization requirements set forth in the applicable law would be of paramount importance for the parties. The contract would not be able to override those requirements.

11. **Data localization requirements** may also arise from third party contractual commitments, e.g., **IP licences** that require the licensed content to be stored on the user's own secured servers. **Data localization** may be preferred for purely practical reasons, for example to reduce **latency**, which may be especially important for real-time operations, such as stock exchange trading. (On contractual data localization safeguards, see part two, paras. 74–75 and 78.)

Choice of a contracting party

12. The choice of a contracting party may be restricted, in addition to market conditions, by statutory requirements. There may be a statutory prohibition on entering into a cloud computing contract with foreign persons, persons from certain jurisdictions or persons not accredited/certified with competent State authorities. There may be a requirement for a foreign person to form a joint venture with a national entity or to acquire local licenses and permissions, including export control permissions, for the provision of **cloud computing services** in a particular jurisdiction. **Data localization** requirements (see paras. 10–11 above) as well as statutory obligations on either party to disclose or provide access to the data and other content to foreign State authorities may also influence the choice of a contracting party.

B. Pre-contractual risk assessment

13. The applicable mandatory law may require a risk assessment as a precondition to entering into a cloud computing contract. Even in the absence of statutory requirements, the parties may decide to undertake a risk assessment that might help them to identify risk mitigation strategies, including the negotiation of appropriate contractual clauses.

14. Not all risks arising from cloud computing contracts would be cloud-specific. Some risks would be handled outside a cloud computing contract (e.g., risks arising from online connectivity interruptions) and not all risks could be mitigated at an acceptable cost (e.g., reputational damage). In addition, risk assessment would not be a one-off event before concluding a contract. Risk assessment could be ongoing throughout the duration of the contract, and risk assessment outcomes may necessitate amendment or termination of the contract.

Verification of information about a specific cloud computing service and a selected contracting party

15. The following information may be relevant to the parties when they consider employing a specific **cloud computing service** and selecting a contracting party:

(a) **IP licenses** required for using a specific cloud computing service;

(b) The privacy, confidentiality and security policies in place, in particular as regards prevention of unauthorized access, use, alteration or destruction of the data during processing, transit or transfer using the cloud computing infrastructure;

(c) Measures in place to ensure the ongoing access to **metadata**, audit trails and other logs demonstrating security measures;

(d) The existing disaster recovery plan and notification obligations in the case of a security breach or system malfunction;

(e) Policies in place as regards migration-to-the-cloud and end-of-service assistance as well as **interoperability** and **portability**;

(f) The existing measures for vetting and training of employees, subcontractors and other third parties involved in the provision of the cloud computing services;

(g) Statistics on **security incidents** and information about past performance with disaster recovery procedures;

(h) Certification by an independent third party on compliance with technical standards;

(i) Information indicating regularity and extent of audit by an independent body;

(j) Financial viability;

(k) Insurance policies;

(l) Possible conflicts of interest;

(m) Extent of subcontracting and **layered cloud computing services**; and

(n) Extent of isolation of data and other content in the cloud computing infrastructure.

IP infringement risks

16. IP infringement risks may arise if, for example, the provider is not the owner or developer of the resources that it provides to its customers, but rather uses them under a **IP licence** arrangement with a third party. IP infringement risks may also arise if the customer is required, for the implementation of the contract, to grant to the provider a licence to use the content that the customer intends to place in the cloud. In some jurisdictions, storage of the content on the cloud even for backup purposes may be qualified as a reproduction and require prior authorization from the IP rights owner.

17. It is in the interests of both parties to ensure before the conclusion of the contract that the use of the cloud computing services would not constitute an infringement of IP rights and a cause for the revocation of the IP licences granted to either of them. Costs of IP infringement may be very high. The right to sublicense may need to be

arranged, or a direct licence arrangement may need to be concluded with the relevant third party licensor under which the right to manage the licences will be granted. The use of open source software or other content may necessitate obtaining an advance consent from third parties and disclosing the source code with any modifications made to open source software or other content.

Risks to data security, integrity, confidentiality and privacy

18. Migration of all or part of data to the cloud leads to the loss of exclusive control by the customer over that data and ability to deploy the necessary measures to guarantee data integrity and confidentiality or verify whether data processing and retention are being handled adequately. The extent of the loss of control will depend on the type of **cloud computing service**.

19. Inherent features of **cloud computing services** such as **broad network access, multi-tenancy** and **resource pooling** may require from the parties more precautions to prevent interception of communications and other cyberattacks, which may lead to the loss or compromise of credentials for access to cloud computing services, data loss and other security breaches. Adequate isolation of resources and data segregation and robust security procedures are especially important in a shared environment such as cloud computing.

20. Security measures will be the shared responsibility of the parties in the cloud computing environment regardless of the type of cloud computing services employed. Pre-contractual risk assessment provides a good opportunity for the parties to eliminate any ambiguity in defining their roles and responsibilities related to data security, integrity, confidentiality and privacy. Contractual clauses will play an important role in reflecting the agreement of the parties on allocation of risks and liabilities between them related to those and other aspects of the provision of cloud computing services (see part two, paras. 125–137). Those clauses will not be able to override mandatory provisions of law.

Penetration tests, audits and site visits

21. Steps may be taken at the pre-contractual stage to verify the adequacy of isolation of resources and data segregation, identification procedures and other security measures. They should aim at identifying possible additional precautions that may need to be taken by the parties to prevent data security breaches and other malfunctions in the provision of the cloud computing services to the customer.

22. Laws and regulations may require **audits**, penetration tests and physical inspection of data centres involved in the provision of the **cloud computing services**, in particular to ascertain that their location complies with statutory **data localization requirements** (see paras. 10–11 above). The parties would need to agree on conditions for undertaking those activities, including their timing, allocation of costs and indemnification for any possible damage caused by those activities.

Lock-in risks

23. Avoiding or reducing **lock-in** risks, often arising from the lack of **interoperability** and **portability,** may be one of the most important considerations for the parties. Higher lock-in risks may arise from long-term contracts and from automatically renewable short- and medium-term contracts.

24. Risks of application and data lock-ins are especially high in **SaaS** and **PaaS**. Data may exist in formats specific to one cloud system that will not be usable in other systems. In addition, a proprietary application or system used to organize data may require adjustment of licensing terms to allow operation in a different network. Programs to interact with the application programming interfaces (API) may need to be rewritten to take into account the new system's API. High switching costs may also arise from the need to retrain end users.

25. In **PaaS**, there could also be runtime lock-in since runtimes (i.e., software designed to support the execution of computer programs written in a specific programming language) are often heavily customized (e.g., aspects such as allocating or freeing memory, debugging, etc.). **IaaS** lock-in varies depending on the specific infrastructure services consumed but may also lead to application lock-in if there is dependence on specific policy features (e.g., access controls) or data lock-in if more data are moved to the cloud for storage.

26. At the pre-contractual stage, tests could be run to verify whether data and other content can be exported to another system and made usable there. Synchronization between cloud and in-house platforms and replication of data elsewhere may be needed. Transacting with more than one party and opting for a combination of various types of **cloud computing services** and their **deployment models** (i.e., multi-sourcing), although possibly with cost and other implications, may be an important part of the mitigating strategy against **lock-in** risks. Contractual clauses may also assist with mitigating lock-in risks (see part two, in particular, paras. 84–85 and 143).

Business continuity risks

27. The parties may be concerned about business continuity risks not only in anticipation of the scheduled termination of the contract, but also of its possible unilateral suspension or earlier termination, including when either party may no longer be in business. The law may require putting in place in advance an appropriate strategy to ensure business continuity, in particular in order to avoid the negative impact of termination or suspension of the cloud computing services on end users. Contractual clauses may also assist with mitigating business continuity risks (see part two, paras. 114–115, 153, 173 and 182).

Exit strategies

28. For successful exit strategies, parties may need to clarify from the outset: (a) the content that will be subject to exit (e.g., only the data that the customer entered in the cloud or also **cloud service-derived data**); (b) any amendments that would be required to **IP licenses** to enable the use of that content in another system; (c) control of decryption keys and access to them; and (d) the time period required to complete the exit. End-of-service contractual clauses usually reflect the agreement of the parties on those issues (see part two, paras. 157–167).

C. Other pre-contractual issues

Disclosure of information

29. The applicable law may require the parties to a contract to provide to each other information that would allow them to make an informed choice about the conclusion of the contract. The absence, or the lack of clear communication to the other party, of information that would make the object of the obligation determined or determinable prior to contract conclusion may make a contract or part thereof null and void or entitle the aggrieved party to claim damages.

30. In some jurisdictions, pre-contractual information may be considered an integral part of the contract. In such cases, the parties would need to ensure that such information is appropriately recorded and that any mismatch between that information and the contract itself is avoided. The parties would also need to deal with concerns over the impact of pre-contractually disclosed information on flexibility and innovation at the contract implementation stage.

Confidentiality

31. Some information disclosed at the pre-contractual stage may be considered confidential, in particular as regards security, identification and authentication measures, subcontractors and the location and type of data centres, which in turn may

identify the type of data stored there and access thereto by local or foreign State authorities. The parties may agree that certain information disclosed at the pre-contractual stage should be treated as confidential. Written confidentiality undertakings or non-disclosure agreements may be required also from third parties involved in pre-contractual due diligence (e.g., auditors).

Migration to the cloud

32. Before migration to the cloud, the customer would usually be expected to classify data to be migrated to the cloud and secure it according to its level of sensitivity and criticality and inform the provider about the level of protection required for each type of data. The customer may also be expected to supply to the provider other information necessary for the provision of the services (e.g., the customer's data retention and disposition schedule, user identity and access management mechanisms and procedures for access to the encryption keys if necessary).

33. In addition to the transfer of data and other content to the provider's cloud, migration to the cloud may involve installation, configuration, encryption, tests and training of the customer's staff and other end users. Those aspects may be part of the customer contract with the provider or be the subject of a separate agreement of the customer with the provider or third parties, such as **cloud computing service partners**. Extra costs may arise. Parties involved in the migration would normally agree on their roles and responsibilities during migration, terms of their engagement, the format in which the data or other content is to be migrated to the cloud, timing of migration, an acceptance procedure to ascertain that the migration was performed as agreed and other details of the migration plan.

Part two. Drafting a contract

A. General considerations

Freedom of contract

34. The widely recognized principle of freedom of contract in business transactions allows parties to enter into a contract and to determine its content. Restrictions on freedom of contracts may stem from legislation on non-negotiable terms applicable to particular types of contract or rules that punish abuse of rights and harm to public order, morality and so forth. The consequences of non-compliance with those restrictions may range from unenforceability of a contract or part thereof to civil, administrative or criminal liability.

Contract formation

35. The concepts of offer and acceptance have traditionally been used to determine whether and when the parties have reached an agreement as regards their respective legal rights and obligations that will bind them over the duration of the contract. The applicable law may require certain conditions to be fulfilled for a proposal to conclude a contract to constitute a final binding offer (e.g., the proposal is to be sufficiently definite as regards the covered cloud computing services and payment terms).

36. The contract is concluded when the acceptance of the offer becomes effective. There could be different acceptance mechanisms (e.g., for the customer clicking a check box on a web page, registering online for a cloud computing service, starting to use cloud computing services or paying a service fee; for the provider starting or continuing to provide services; and for both parties signing a contract online or on paper). Material changes to the offer (e.g., as regards liability, quality and quantity of the cloud computing services to be delivered or payment terms) may constitute a counteroffer that requires acceptance by the other party for a contract to be concluded.

37. **Standardized commoditized multi-subscriber cloud solutions** are as a rule offered through interactive applications (e.g., "click-wrap" agreements). There may be no or very little room for negotiating and adjusting the standard offer. Clicking "I accept", "OK" or "I agree" is the only step expected to be taken to conclude the contract. Where negotiation of a contract is involved, contract formation may consist of a series of steps, including preliminary exchange of information, negotiations, delivery and acceptance of an offer and the contract's preparation.

Contract form

38. Cloud computing contracts are typically concluded online. They may be called differently (a cloud computing service agreement, a master service agreement or terms of service (TOS)) and may comprise one or more documents such as an **acceptable use policy (AUP)**, a **service level agreement (SLA)**, a data processing agreement or data protection policy, security policy and license agreement.

39. The legal rules applicable to cloud computing contracts may require that the contract be in **writing**, especially where **personal data processing** is involved, and that all documents incorporated by reference be attached to the master contract. Even when **written** form is not required, for ease of reference, clarity, completeness, enforceability and effectiveness of the contract, the parties may decide to conclude a contract in **writing** with all ancillary agreements incorporated thereto.

40. The signing of a contract on paper may be required under the applicable law for specific purposes such as tax purposes, although that type of requirement is becoming rare in the paperless environment.

Definitions and terminology

41. Due to the nature of **cloud computing services**, cloud computing contracts contain by necessity many technical terms. The glossary of terms may be included in the contract, as may definitions of main terms used throughout the contract, to avoid ambiguities in their interpretation. The parties may wish to consider using the internationally established terminology for the purpose of ensuring consistency and legal clarity.

Minimum contract content

42. A contract normally: (a) identifies the contracting parties; (b) defines the scope and object of the contract; (c) specifies rights and obligations of the parties, including payment terms; (d) establishes the duration of the contract and conditions for its termination and renewal; (e) identifies remedies for breach and exemptions from liability; and (f) specifies the effects of the termination of the contract. It also usually contains clauses on dispute resolution and choice of law and choice of forum.

B. Identification of contracting parties

43. The correct identification of contracting parties may have a direct impact on the formation and enforceability of the contract. The applicable law would specify the information needed to ascertain the legal personality of a business entity and its capacity to enter into a contract. The law may require additional information for specific purposes, for example, an identification number for tax purposes or power of attorney to ascertain the power of a natural person to sign and commit on behalf of a legal entity.

C. Defining the scope and the object of the contract

44. Objects of cloud computing contracts vary substantially in their type and complexity given the range of **cloud computing services**. Within the duration of a single contract, the object may change: some **cloud computing services** may be cancelled and other services may be added. The object of the contract may comprise the provision of core, ancillary and optional services.

45. The description of the object of the contract usually includes a description of a type of cloud computing services (**SaaS, PaaS, IaaS** or a combination thereof), their **deployment model** (**public, community, private** or **hybrid**), their technical, quality and performance characteristics and any applicable technical standards. Several documents comprising the contract may be relevant for determining the object of the contract (see para. 38 above).

Service level agreement

46. The **service level agreement (SLA)** contains **performance parameters** against which the delivery of the cloud computing services, the extent of the contractual obligations and possible contractual breaches of the provider will be measured. Information technology specialists are normally involved in the formulation of the **performance parameters.**

47. Quantitative performance parameters usually relate to capacity (a specified capacity of data storage or specified amount of memory available to the running program), **downtime** or **outages**, **latency**, **persistency of data storage**, **uptime**, support services (e.g., during the customer's operating hours or 24/7), and incident and disaster management and recovery plans. The latter may include the maximum incident resolution time, the maximum **first response time**, **recovery point objectives** and **recovery time objectives**.

48. Qualitative performance parameters may relate to **data deletion**, **data localization requirements**, **portability**, security and data protection/privacy. Some

aspects of service may be measured against both qualitative and quantitative performance parameters. For example, **elasticity** and **scalability** may be defined with reference to both the maximum available resources within a specified minimum period and the quality and security of the measures that may need to be adapted to the varying degrees of sensitivity of the stored customer data. Encryption may be expressed as a defined bit value at rest, in transit and in use. In addition to or instead of such a quantitative parameter, encryption may be measured against a qualitative parameter (e.g., the provider is to ensure that customer data are encrypted whenever they are transported over a public communication network and whenever they are at rest in data centres used by the provider).

49. Different commitments (i.e., obligations of result or of best efforts) could be agreed upon depending in particular on the terms of payment and whether **standardized commoditized multi-subscriber solutions** are provided. The type of commitment would have implications, including for the burden of proof in case of dispute.

Performance measurement

50. The parties may include in the contract a measurement methodology and procedures, specifying in particular a reference period for the measurement of services (daily, weekly, monthly, etc.), service delivery reporting mechanisms (i.e., the frequency and form of such reporting), the role and responsibilities of the parties and metrics to be used (e.g., metrics at the point of provision or at the point of consumption of services). The parties may agree on an independent measurement of performance and how the related costs are to be allocated.

51. The customer is normally interested in measuring services during peak hours, i.e., when they are most needed. The customer is usually able to measure, or verify the measurements provided by the provider or third parties, of only those metrics that are based on performance at the point of consumption, but not those based on system performance at the point of provision of services. The customer may be able to evaluate the performance at the point of provision of services based on reports provided by the provider or third parties. The provider may agree to provide the customer with performance reports on demand, periodically (daily, weekly, monthly, etc.) or following a particular incident. Alternatively, the provider may agree to grant the customer the right to review the provider's records related to the service-level measurements. Some providers enable customers to monitor data on service performance in real time.

52. The contract may oblige either or both parties to maintain records about the provision and consumption of services for a certain length of time. Such information may be useful in negotiating any amendments to the contract and in case of disputes.

Acceptable use policy

53. An **acceptable use policy (AUP)** sets out conditions for use by the customer and its end users of the cloud computing services covered by the contract. It aims at protecting the provider from liability arising out of the conduct of their customers and customers' end users. Any potential customer is expected to accept such a policy, which will form part of the contract with the provider. The vast majority of standard **AUPs** prohibit a consistent set of activities that providers consider to be improper or illegal uses of **cloud computing services**. The **AUP** may restrict not only the type of content that may be placed on the cloud but also the customer's right to give access to data and other content placed on the cloud to third parties (e.g., nationals of certain countries or persons included in sanctions lists). The parties may agree to remove some prohibitions to accommodate specific business needs of the customer to the extent that such removal would be permissible under law.

54. It is usual for provider's standards terms to require that customer's end users also comply with the **AUP** and to oblige the customer to use its best efforts or commercially reasonable efforts to ensure such compliance. Some providers may

require customers to affirmatively prevent any unauthorized or inappropriate use by third parties of the cloud computing services offered under the contract. The parties may agree on limited obligations, for example, that the customer will communicate the **AUP** to known end users, not authorize or knowingly allow such uses, and notify the provider of all unauthorized or inappropriate uses of which it becomes aware.

55. In a few jurisdictions, the law could impose duties on the provider as regards the content hosted on its cloud computing infrastructure, e.g., the duty to report illegal material to public authorities. Those duties may be non-transferrable to the customer or to end users by the **AUP** or otherwise. They might have privacy and other ramifications and would be among factors considered in choosing a suitable provider (see part one, para. 12).

Security policy

56. Security of the system, including customer data security, involves shared responsibilities of the parties. The contract would need to specify reciprocal roles and responsibilities of the parties as regards security measures, reflecting obligations that may be imposed by mandatory law on either or both parties.

57. Usually, the provider will follow its security policies. In some cases, although not in **standardized commoditized multi-subscriber solutions**, it might be possible to reach an agreement that the provider will follow the customer's security policies. The contract may specify security measures (e.g., requirements for sanitization or deletion of data in the damaged media, the storage of separate packages of data in different locations, the storage of the customer's data on specified hardware that is unique to the customer). Excessive disclosure of security information in the contract may, however, be risky.

58. Some security measures do not presuppose the other party's input but rely exclusively on the relevant party's routine activities, such as inspections by the provider of the hardware on which the data is stored and on which the services run, and effective measures to ensure controlled access thereto. In other cases, allowing the party to perform its duties or evaluate and monitor the quality of security measures delivered may presuppose the input of the other party. The customer, for example, would be expected to update lists of users' credentials and their access rights and inform the provider of changes in time to ensure the proper identity and access management mechanisms. The customer would also be expected to inform the provider about the level of security to be allocated to each category of data.

59. Some threats to security may be outside the contractual framework between the customer and the provider and may require the terms of the cloud computing contract to be aligned with other contracts of the provider and the customer (e.g., with Internet service providers).

Data integrity

60. Providers' standard contracts may contain a general disclaimer that the ultimate responsibility for preserving the integrity of the customer's data lies with the customer.

61. Some providers may be willing to undertake data integrity commitments (for example, regular backups), possibly for an additional payment. Regardless of the contractual arrangements with the provider, the customer may wish to consider whether it is necessary to secure access to at least one usable copy of its data outside the provider's and its subcontractors' control, reach or influence and independently of their participation.

Confidentiality clause

62. The provider's willingness to commit to ensuring the confidentiality of customer data depends on the nature of services provided to the customer under the contract, in particular whether the provider will be required to have unencrypted

access to data for the provision of those services. Some providers may not be in a position to offer a confidentiality or non-disclosure clause and may expressly waive any duty of confidentiality regarding customer data. Other providers may be willing to assume liability for confidentiality of data disclosed by the customer during contract negotiations, but not for data processed during service provision. Some standard confidentiality clauses offered by providers may not be sufficient to ensure compliance with applicable law.

63. In the absence of contractual commitments and statutory obligations on the provider to maintain confidentiality, the customer may have full responsibility for keeping data confidential, e.g., through encryption. Where the possibility of negotiating a general confidentiality clause applicable to all customer data placed in the cloud does not exist, the parties may agree on confidentiality commitments as regards some sensitive data (with a separate liability regime for breach of confidentiality of such data). The customer may in particular be concerned about its trade secrets, know-how and information that it is required to keep confidential under law or commitments to third parties. The parties may agree to restrict access to such data to a limited set of personnel and to require individual confidentiality commitments from them, in particular from those with high-risk roles (e.g., system administrators, auditors and persons dealing with intrusion detection reports and incident response). In those cases, the customer would normally specify to the provider such information, the required level of protection, any applicable law or contractual requirements and any changes affecting such information, including any changes in the applicable legislation.

64. In some cases, the disclosure of customer data may be necessary for the fulfilment of the contract. In other cases, the disclosure may be mandated by law, for example, under the duty to provide information to competent State authorities (see para. 82 below). Appropriate exceptions to confidentiality clauses would thus be warranted.

65. The provider may in turn impose on the customer the obligation not to disclose information about the provider's security arrangements and other details of services provided to the customer under the contract or law.

Data protection/privacy policy or data processing agreement

66. **Personal data** are subject to special protection by law in many jurisdictions. Law applicable to **personal data processing** may be different from the law applicable to the contract. It will override any non-compliant contractual clauses.

67. The contract may include a data protection or privacy clause, data processing agreement or similar type of agreement, although some providers may agree only to the general obligation to comply with applicable data protection laws. In some jurisdictions, such general commitment may be insufficient: the contract would need to stipulate at a minimum the subject matter and the duration, nature and purpose of the **personal data processing**, the type of **personal data** and categories of **data subjects** and the obligations and rights of the **data controller** and the **data processor**. Where the possibility of negotiating a data protection clause in the contract does not exist, the customer may wish to review standard terms to determine whether the provisions give the customer sufficient guarantees of lawful **personal data processing** and adequate remedies for damages.

68. The customer will likely be the **data controller** and will assume responsibility for compliance with the data protection law in respect of **personal data** collected and processed in the cloud. The parties may agree on contractual clauses aimed at ensuring compliance with the applicable data protection regulations, including requests related to the **data subjects' rights.** The parties may also agree on separate remedies should those clauses be breached, including unilateral termination of the contract and compensation for damages.

69. Providers' standard contracts usually stipulate that the provider does not assume any **data controller** role. The provider will likely act as the **data processor** only when it processes the customer's data according to instructions of the customer for the sole purpose of providing the cloud computing services. The provider may, however, be regarded as the **data controller** in some jurisdictions, regardless of contractual clauses, when it further processes data for its own purposes or upon instructions of State authorities and could thus assume full responsibility for **personal data** protection in respect of that further **personal data processing** (see para. 125 below).

Obligations arising from data breaches and other security incidents

70. The parties may be required under law or contract or both to notify each other immediately of a **security incident** of relevance to the contract or any suspicion thereof that becomes known to them. That obligation may be in addition to general notification of a security incident that may be required under law to inform all relevant stakeholders, including **data subjects**, insurers and State authorities, or the public at large, in order to prevent or minimize the impact of security incidents.

71. The law may contain specific security incident notification requirements, including the timing of notification, and identify the persons responsible for complying with them. Subject to those mandatory provisions, the parties may specify in the contract the notification period (e.g., one day after the party becomes aware of the incident or threat), the form and content of the security incident notification. The latter usually includes circumstances and the cause of the incident, type of affected data, the steps to be taken to resolve the incident, the time at which the incident is expected to be resolved and any contingency plan to employ while the incident is being resolved. It may also include information on failed breaches, attacks against specific targets (per customer user, per specific application, per specific physical machine), trends and statistics. Any notification requirements normally take into account the need not to disclose any sensitive information that could lead to the compromise of the affected party's system, operations or network.

72. The provider, the customer, or both, including by involving a third party, may be required by law or contract to take measures after a security incident (so-called "post-incident steps"), including the isolation or quarantine of affected areas, the performance of root cause analysis and the production of an incident analysis report. The incident analysis report may be produced by the affected party or by the affected party jointly with the other party or by an independent third party. Post-incident steps may vary depending on the categories of data stored in the cloud and other factors.

73. A serious security incident resulting in, for example, a loss of data may lead to the termination of the contract.

Data localization requirements

74. Providers' standard terms may expressly reserve the right of the provider to store customer data in any country in which the provider or its subcontractors operate. Such a practice will most likely be followed even in the absence of an explicit contractual right, since it is implicit in the provision of **cloud computing services** that they are provided, as a general rule, from more than one location (e.g., backup and antivirus protection may be remote, and support may be provided in a global "**follow-the-sun**" model). That practice may not comply with **data localization requirements** applicable to either or both parties (see part one, paras. 10–11).

75. Safeguards ensuring compliance with **data localization requirements** may be included in the contract, such as a prohibition on moving data and other content outside the specified location or a requirement of prior approval of such moves by the other party. For example, an **SLA** qualitative performance parameter may be included to ensure that the customer data (including any copy, **metadata** and backup thereof) would be stored exclusively in data centres physically located in the jurisdictions indicated in the contract and owned and operated by entities established in those

jurisdictions. Alternatively, the parameter may specify, for example, that data should never be moved outside a specific country or region but may be duplicated in a particular third country or elsewhere, but never in a specific country.

D. Rights to customer data and other content

Provider rights to customer data for the provision of services

76. Providers usually reserve the right to access customer data on a "need-to-know" basis. That arrangement would allow access to customer data by the provider's employees, subcontractors and other third parties (e.g., auditors) where necessary for the provision of the cloud computing services (including maintenance, support and security purposes) and for monitoring compliance with applicable **AUP, IP licences, SLA** and other contractual documents. The parties may agree on circumstances when the provider's access to customer data would be allowed and measures that would ensure confidentiality and integrity of customer data.

77. Certain rights to access customer data can be considered to be implicitly granted by the customer to the provider by requiring a certain service or feature: without those rights, the provider would not be able to perform the services. For example, if the provider is required to regularly back up customer data, the fulfilment of that task necessitates the right to copy the data. Likewise, if subcontractors are to handle customer data, the provider must be able to transfer the data to them.

78. The contract may explicitly indicate which rights concerning data required for the performance of the contract the customer grants to the provider, whether and to what extent the provider is entitled to transfer those rights to third parties (e.g., its subcontractors) and the geographical and temporal extent of the granted or implied rights. The geographical limitations could be particularly important when data cannot leave a certain country or region under law (see part one, paras. 10–11). Contracts typically state whether the customer is able to revoke granted or implied rights and if so, under what conditions. Since the ability to provide the services at the required level of quality may depend on the rights granted by the customer, the direct impact of revocation of certain rights could be the amendment or termination of the contract.

Provider use of customer data for other purposes

79. Most jurisdictions do not grant the provider automatic rights to use the customer data for the provider's own purposes. The provider may request use of customer data for purposes other than those linked to the provision of the cloud computing services under the contract (e.g., for advertising, generating statistics, analytical or predictions reports, engaging in other data mining practice). The questions to consider in that context may include: (a) which information about the customer and its end users will be collected and the reasons for and purposes of its collection and use by the provider; (b) whether that information will be shared with other organizations, companies or individuals and if so, the reasons for doing so and whether this will be done with or without the customer's consent; and (c) how compliance with confidentiality and security policies will be ensured if the provider shares that information with third parties. Where the provider's use of customer data will affect **personal data**, the parties would normally be expected to carefully assess their regulatory compliance obligations under applicable data protection laws.

80. Where the contract gives the provider rights to use the customer data for the provider's own purposes, the contract may also list permissible grounds for such use, include obligations regarding de-identification and anonymization of customer data to ensure compliance with any applicable data protection and other regulations and impose limits on reproduction of content and communication to public. It is common to permit the provider to use customer data for its own purposes only as anonymized open data or in aggregated and de-identified form during the term of the contract or beyond.

Provider use of customer name, logo and trademark

81. The providers' standard terms may grant the provider the right to use customer names, logos and trademarks for the purposes of the provider's publicity. The parties may agree on the deletion or modification of such provisions, including limiting the permissible use to the customer's name and seeking the prior approval of the customer for the use of its name, logo and trademark.

Provider actions as regards customer data upon State orders or for regulatory compliance

82. The provider' standard terms may reserve the right for the provider, at its discretion, to disclose, or provide access to, customer data to State authorities (e.g., by including such wording as "when doing so will be in the best interests of the provider"). They also usually provide for the right of the provider to remove or block customer data immediately after the provider gains knowledge or becomes aware of illegal content or when it has to enforce **the right of data subjects to be forgotten**, in order to avoid liability under law (the "notice and take down" procedure (see para. 128 below)). The parties may agree to narrow down the circumstances in which the provider can perform those actions, for example when the provider faces an order from a court or other State authority to provide access to, or to delete or change, data.

83. The parties may agree, at a minimum, that the customer will be notified without delay of State orders or the provider's own decisions as regards customer data with a description of the data concerned, unless such notification would violate law. Where the advance notification and involvement of the customer is not possible, the contract may require the provider to serve an immediate ex-post notification to the customer of the same information. The parties may also agree on provisions as regards keeping and providing customer access to and logs of all orders, requests and other activities as regards customer data.

Rights to cloud service-derived data

84. The parties may agree on customer rights to **cloud service-derived data** and how such rights can be exercised during the contractual relationship and upon termination of the contract.

IP rights protection clause

85. Some types of cloud computing contracts may result in the creation of objects of IP rights, either jointly by the provider and the customer (e.g., service improvements arising from the customer's suggestions) or by the customer alone (new applications, software and other original work). The contract may contain an express IP clause that will determine which party to the contract owns IP rights to various objects deployed or developed in the cloud and the use that the parties can make of such rights. Where no option to negotiate exists, the customer may wish to review any IP clauses to determine whether the provider offers sufficient guarantees and allows the customer appropriate tools to protect and enjoy its IP rights and avoid **lock-in** risks (see part one, paras. 23–26).

Interoperability and portability

86. There may be no statutory requirements to ensure **interoperability** and **portability**. The onus might be completely on the customer to create compatible export routines, unless the contract provides otherwise, for example, by including contractual commitments as regards interoperability and portability and assistance with the export of data upon termination of the contract (see para. 161 below). The contract may require the use of common, widely used standardized or interoperable export formats for data and other content or provide choice among available formats. Contractual clauses may also be included to address rights to joint products and applications or software, without which the use of the data and other content in another system may be impossible (see para. 85 above).

Data retrieval for legal purposes

87. Customers may be required to be able to search and find data placed in the cloud in its original form for legal purposes, for example, in investigations. The electronic records may need to meet auditing and evidentiary standards. Some providers may be in a position to offer customers assistance with the retrieval of data in the format required by law. The contract may define the form and terms of such assistance.

Data deletion

88. **Data deletion** considerations may be applicable during the term of the contract, but particularly upon its termination (see para. 162 below). For example, certain data may need to be deleted according to the customer's retention plan. Sensitive data may need to be destroyed at a specified time in its lifecycle (e.g., the destruction of hard disks at the end of the life of equipment on which such data was stored). Data may also need to be deleted in order to comply with law enforcement deletion requests or after confirmed IP infringement cases (see para. 82 above).

89. The provider' standard terms may contain only statements to delete customer data from time to time. The parties may agree on the deletion of data, its backups and **metadata** immediately, effectively, irrevocably and permanently, in compliance with the data retention and disposition schedules or other form of authorization or request communicated by the customer to the provider. The contract may address the time period and other conditions for data deletion, including obligations as regards a confirmation of the data deletion upon its completion and access to audit trails of the deletion activities.

90. Particular standards or techniques for deletion may be specified, depending on the nature and sensitivity of the data. It may be required to delete data from different locations and media, including from subcontractors' and other third parties' systems, with different levels of deletion, such as data sanitization ensuring confidentiality of the data until their complete deletion or hardware destruction. More secure deletion involving destruction rather than redeployment of equipment may be more expensive and may not always be possible (if, for example, data of other persons is stored on the same hardware). Those aspects may trigger the inclusion of contractual requirements to use an isolated infrastructure for storing the customer's particularly sensitive data.

E. Audits and monitoring

Monitoring activities

91. The parties may need to monitor activities of each other to ensure regulatory and contractual compliance (e.g., compliance of the customer and its end users with **AUP** and **IP licenses** and compliance of the provider with **SLA** and data protection policy). Some monitoring activities, such as those related to **personal data processing,** may be mandated by law.

92. The contract may identify periodic or recurrent monitoring activities, together with the party responsible for their performance and the obligations of the other party to facilitate monitoring. The contract may also anticipate any exceptional monitoring activities and provide options for handling them. The contract may also provide for reporting requirements to the other party as well as any confidential undertakings in conjunction with such monitoring activities.

93. Excessive monitoring may affect performance and increase costs of services. The contract may provide for the requirement to suspend monitoring in certain circumstances, e.g., where monitoring is materially detrimental to the service performance. That concern may be present particularly in case of services requiring near real-time performance.

Audit and security tests

94. Audit and security tests, in particular to check the effectiveness of security measures, are common. Some audits and security tests may be mandated by law. The contract may include clauses that address the audit rights of both parties, the scope of audits, recurrence, formalities and costs. It may also oblige the parties to share with each other the results of the audits or security tests that they commission. The contractual rights or statutory obligations for audit and security tests may be complemented in the contract with corresponding obligations of the other party to facilitate the exercise of such rights or fulfilment of those obligations (e.g., to grant access to the relevant data centres).

95. Parties may agree that audits or security tests may be performed only by professional organizations or that the provider or the customer may choose to have the audit or security test performed by a professional organization. The contract may specify qualifications to be met by the third party and conditions for their engagement, including allocation of costs. Special arrangements may be agreed upon by the parties for audits or security tests subsequent to an incident and depending on the severity and type of the incident (for example, the party responsible for the incident may be obliged to partially or fully reimburse costs).

F. Payment terms

Pay-as-you-go

96. Price is an essential contractual term, and failure to include the price or a mechanism for determining the price in the contract may render the contract unenforceable.

97. The **on-demand self-service** characteristic of cloud computing services is usually reflected in the **pay-as-you-go** billing system. It is common for the contract to specify the price per unit for the agreed volume of supply of the cloud computing services (e.g., for a specified number of users, number of uses or time used). Price scales or other price adjustments, including volume discounts, may be designed as incentives or penalties for either of the parties. Free trials are common. It is also common not to charge for some services. Although there could be many variations for price calculation, a clear and transparent price clause, understood by both parties, may avoid conflict and litigation.

Licensing fees

98. The parties may wish to clarify in the contract whether the payment for the cloud computing services encompasses licensing fees for any licences the provider may grant to the customer as part of the services. **SaaS**, in particular, often involves the use by the customer of software licensed by the provider.

99. The licensing fees may be calculated on a per-seat or per instance basis and fees may vary depending on the category of users (e.g., professional users, as opposed to non-professional users, may fall in one of the most expensive categories). Different payment structures may have different implications. For example, a customer's licence costs may increase exponentially if software is charged on a per instance basis each time a new machine is connected, even though the customer is using the same number of machine instances for the same duration.

100. The contract may identify the total number of potential users of software covered by the licence arrangement, the number of users in each category (e.g., employees, independent contractors and suppliers) and the rights to be granted to each category of users. The contract may also identify access and use rights that will be included in the scope of the licence and cases of access and use by the customer and its end users that may lead to an expanded scope of the license and consequently to increased licensing fees.

Additional costs

101. The price may cover also one-off costs (e.g., configuration and migration to the cloud (see part one, paras. 32–33). There could also be additional services offered by the provider against separate payment (e.g., support after business hours charged per time or provided for a fixed price).

102. Whether cloud computing services fall within the category of taxable services or goods would depend on jurisdictions. The parties may wish to address in the contract the impact of taxes on payment terms.

Other payment terms

103. Payment terms may cover invoicing modalities (e.g., e-invoicing) and the form and content of the invoice, which may be important for tax compliance. Tax authorities of some jurisdictions may not accept electronic invoices (although this is becoming rare in the paperless environment) or may require a special format, including that any tax applicable to the cloud computing services may need to be stated separately.

104. The parties may wish to include, among other payment terms, payment due date, currency, the applicable exchange rate, manner of payment, sanctions in case of late payment and procedures for resolving disputes over payment claims.

G. Changes in services

105. **Cloud computing services** are by nature flexible and fluctuating. The **elasticity**, **scalability** and **on-demand self-service** characteristics of **cloud computing services** are usually enabled through many contractual options that the customer may use to adjust the consumption of services according to its needs. This prevents the need for renegotiation of the contract each time the customer requires a change in the consumption of services.

106. The provider in turn may reserve the right to adjust its service portfolio at its discretion. Different contractual treatment may be appropriate depending on whether changes concern the core services or ancillary services and support aspects. Different contractual treatment may also apply to changes that might negatively affect services as opposed to changes that lead to service improvements (e.g., a switch from a standard offering to an enhanced cloud computing offering with higher security levels or shorter response times). The consequences of some unilateral changes of the terms and conditions of the contract by the provider may be severe for the customer, in particular translating into high costs of migration to another system.

Changes in price

107. The provider may reserve the right to unilaterally modify the price or price scales. The parties may agree to specify in the contract the pricing methodology (e.g., how frequently the provider can increase prices and by how much). The prices may be capped to a specific consumer price index, to a set percentage or to the provider's price list at a given moment. The contract may provide for advance notice of a price increase and the consequences of non-acceptance of the price increase by the customer.

Upgrades

108. Although upgrades may be in the customer's interests, they may also cause disruptions in the availability of cloud computing services since they could translate into relatively high **dowutime** during normal working hours even if the service is to be provided on 24/7 basis. The parties may agree on advance notification to the customer of pending upgrades and the implications thereof and that upgrades, as a rule, will take place during periods of little or no demand for the customer. The contract may also provide for procedures for reporting and solving possible problems.

109. Upgrades may have other negative impacts, for example, requiring changes to customer applications or information technology systems or the retraining of customer users. The contract may provide for the allocation of the costs arising from upgrades. The parties may also agree that the older version of the provided service should be retained in parallel with the new version for an agreed period of time in cases where significant changes are to be made to the previous version, in order to ensure the customer's business continuity. The contract may also address assistance that may be offered by the provider with changes to customer applications or information technology systems and with retraining of the customer's end users, when required.

Degradation or discontinuation of services

110. Technological developments, competitive pressure or other causes may lead to the degradation of some cloud computing services or their discontinuation with or without their replacement by other services. The provider may reserve in the contract the right to adjust the service portfolio offering, e.g., by terminating a portion of the services. Discontinuation of even some cloud computing services by the provider may, however, expose the customer to liability to its end users.

111. The contract may provide for an advance notification of those changes to the customer, the customer's right to terminate the contract in the case of unacceptable changes and an adequate retention period to ensure the timely **reversibility** of any affected customer data or other content. Some contracts prohibit modifications that could negatively affect the nature, scope or quality of provided services, or limit permissible changes to "commercially reasonable modifications".

Notification of changes

112. The providers' standard terms may contain an obligation on the provider to notify the customer about changes in the terms of services. If not, customers may be required to check regularly whether there have been any changes in the contract. Documents forming the contract may be numerous (see para. 38 above). Some may incorporate by reference terms and policies contained in other documents, which may in turn incorporate by reference additional terms and policies, all of which may be subject to unilateral modification by the provider. Those different documents may not necessarily be hosted in one place on the provider's website. Changes introduced by the provider to the contract may therefore not be easy to notice.

113. Since the continued use of services by the customer is deemed to be acceptance of the modified terms, the parties may agree that the customer will be notified of changes in the terms of services sufficiently in advance of their effective date. The parties may also agree that the customer will have access to audit trails concerning the evolution of services and that all agreed terms and the definition of the services by reference to a particular version or release will be preserved.

H. Suspension of services

114. The providers' standard terms may contain the right of the provider to suspend services, at its discretion, at any time. "Unforeseeable events" is a common justification for unilateral suspension of services by the provider. Such events are usually defined as broadly encompassing any impediments beyond the provider's control, including failures of subcontractors, sub-providers and other third parties involved in the provision of the cloud computing services to the customer, such as Internet network providers.

115. The parties may agree that suspension of services may occur only in limited cases identified in the contract (e.g., in case of the fundamental breach of the contract by the customer, for example, non-payment). The right of suspension due to unforeseeable events may be conditioned on properly implementing a business continuity and disaster recovery plan. The contract may require that such a plan

contains protections against common threats to the provision of the cloud computing services and be submitted for comment and approval by the other party. Those protections may include a geographically separate disaster recovery site with seamless transition and the use of an uninterruptible power supply and backup generators.

I. Subcontractors, sub-providers and outsourcing

Identification of the subcontracting chain

116. Subcontracting, **layered cloud computing services** and outsourcing are common in cloud computing environment. The providers' standard terms may explicitly reserve the provider's right to use third parties for the provision of the cloud computing services to the customer, or that right may be implicit because of the nature of services to be provided. The provider may be interested in retaining as much flexibility as possible in that respect.

117. The law may require the parties to identify in the contract third parties involved in the provision of the cloud computing services. Such identification may also be beneficial to the customer for verification purposes, in particular of compliance of third parties with security, confidentiality, data protection and other requirements arising from the contract or law and of the absence of conflicts of interest on the part of third parties.

118. That information may also be used for mitigation of risks of non-performance of the contract by the provider due to failures of third parties. For example, the customer may opt to contract directly with third parties instrumental to the performance of the cloud computing contract, in particular on such sensitive issues as confidentiality and **personal data processing**. The customer may also try to negotiate with key third parties obligations to step in if the provider fails to perform under the contract, including in case of the provider's insolvency.

119. The provider may be in a position to identify those third parties playing key roles but not all third parties. The pool of third parties involved in the provision of cloud computing services may change during the contract (see paras. 120–121 below).

Changes in the subcontracting chain

120. Unilateral changes in the subcontracting chain are common. The contract may specify whether changes in the subcontracting chain are permitted and if so, under which conditions, e.g., the customer may reserve the right to vet and veto any new third party involved in the provision of the cloud computing services to the customer before the change is implemented. Alternatively, the contract may include the list of third parties pre-approved by the customer, from which the provider can choose when the need arises. Another option is to subject the change to subsequent approval by the customer, in the absence of which services would need to continue with the previous or other pre-approved third party or with another third party to be agreed by the parties. Otherwise, the contract may be terminated.

121. Mandatory applicable law may stipulate circumstances in which changes in a provider's subcontracting chain may require termination of the contract.

Alignment of contract terms with linked contracts

122. The law or the contract may require the parties to align the terms of the contract with existing or future linked contracts to ensure confidentiality and compliance with **data localization** and data protection requirements. The contract may oblige parties to supply each other with copies of linked contracts for verification purposes.

Liability of subcontractors, sub-providers and other third parties

123. Although third parties instrumental to the performance of the cloud computing contract may be listed in the contract, they would not be parties to the contract between the provider and the customer. They would be liable for obligations under their contracts with the provider. The creation of third party beneficiary rights for the benefit of the customer in linked contracts or making the customer a party to linked contracts would allow the customer's direct recourse against the third party in case of that third party's non-performance under a linked contract.

124. Under applicable law or contract, the provider may be held liable to the customer for any issue within the responsibility of any third party whom the provider involved in the performance of the contract. In particular, the joint liability of the provider and its subcontractors may be established by law for any issues arising from **personal data processing**, depending on the extent of subcontractors' involvement in processing.

J. Liability

Statutory limitations to contractual freedom

125. While most legal systems generally recognize the right of contracting parties to allocate risks and liabilities and limit or exclude liability through contractual provisions, this right is usually subject to various limitations and conditions. For example, an important factor in risk and liability allocation in **personal data processing** is the role that each party assumes as regards the **personal data** placed in the cloud. The data protection law of certain jurisdictions imposes more liability on the **data controller** than on **data processors** of **personal data**. Notwithstanding contractual provisions, the factual handling of such data will generally determine the legal regime to which the party would be subject under applicable law. **Data subjects** who have suffered loss resulting from an unlawful processing of **personal data** or any act incompatible with domestic data protection regulations may be entitled to compensation directly from the **data controller**.

126. In addition, in many jurisdictions a total exclusion of liability for a person's own fault is not admissible or is subject to limitations. It might not be possible to exclude altogether liability related to personal injury (including sickness and death) and for gross negligence, intentional harm, defects, breach of core obligations essential for the contract or non-compliance with applicable regulatory requirements. Some types of limitation clauses, such as waiver of liability by the provider for **security incidents** in cases where the customer has no control or ability to effect security, may be found to be "abusive" and therefore invalid. The terms of contracts of adhesion, which are typically not negotiated but pre-established by one of the parties, may be subject to particular scrutiny. In addition, unlimited liability may flow from certain types of defects under law (e.g., defective hardware or software).

127. The ability of public institutions to assume certain liabilities may be restricted by law, or public institutions would need to seek prior approval of a competent State body for doing so. They may also be prohibited from accepting exclusion or limitation of a provider's liability altogether or for acts or omissions defined in law.

128. The applicable law may, on the other hand, provide for exemption from liability if certain criteria are fulfilled by a party that would otherwise face a risk of liability. For example, under the "notice and take down" procedure in some jurisdictions, the provider will be released from liability for hosting the illegal content on its cloud infrastructure if it removed such content once it became aware of it.

129. In some jurisdictions, to be enforceable, the clauses containing disclaimers and limitations of liability agreed upon by the parties must be included in the contract. The applicable law might impose form or other requirements for the validity and enforceability of those clauses.

Other considerations for drafting liability clauses

130. The amount, if any, charged for the cloud computing services and the risks involved in the provision of the services would all be considered in negotiating the allocation of risks and liabilities. Although parties generally tend to exclude or limit liability as regards factors that they cannot control or can control only to a limited extent (e.g., behaviour of end users, actions or omissions of subcontractors), the level of control would not always be a decisive consideration. A party may be prepared to assume risks and liability for elements that it does not control in order to distinguish itself in the market place. It is nevertheless likely that the party's risks and liabilities would increase progressively in proportion to the components under its control.

131. For example, in **SaaS** involving the use of standard office software, it is likely that the provider would be responsible for virtually all resources provided to the customer, and liability of the provider could arise in each case of non-provision or malfunctioning of those resources. Nevertheless, even in those cases, the customer could still be responsible for some components of the services, such as encryption or backups of data under its control. The failure to ensure adequate backups might lead to the loss of the right of recourse against the provider in case of the loss of data. On the other hand, in **IaaS** and **PaaS**, the provider could be responsible only for the infrastructure or platforms provided (such as hardware resources, operating system or middleware), while the customer would assume responsibility for all components belonging to it, such as applications run using the provided infrastructure or platforms and data contained therein.

Provider's standard terms

132. Providers' standard terms may exclude any liability under the contract and take the position that liability clauses are non-negotiable. Alternatively, the provider may be willing to accept liability, including unlimited liability, for breaches controllable by the provider (e.g., a breach of IP licenses granted to the provider by the customer) but not for breaches that may occur for reasons beyond the provider's control (e.g., unforeseeable events or leaks of confidential data).

133. Providers' standard terms generally exclude liability for indirect or consequential loss (e.g., loss of business opportunities following the unavailability of the cloud computing service). Where liability is accepted generally or for certain specified cases, providers' standard terms often limit the amount of losses that will be covered (per incident, per series of incidents or per period of time). In addition, providers often fix an overall cap on liability under the contract, which may be linked to the revenue expected to be received under the contract, to the turnover of the provider or insurance coverage.

134. Providers' standard terms usually impose liability on the customer for non-compliance with the **AUP**.

Possible variations of standard terms

135. Some events (e.g., personal data protection violations and IP rights infringement) could expose either party to the potentially high liability to third parties or give rise to regulatory fines. It is common therefore to agree on a more stringent liability regime (unlimited liability or higher compensation) when those events occur due to the fault or negligence of the other party.

136. On the other hand, liability of the parties for actions of third parties that they cannot control (e.g., of the customer for actions of end users or of the provider for actions of the customer or its end users) may be limited or excluded by contract or law.

Liability insurance

137. The contract may contain insurance obligations for both or either party, in particular as regards quality requirements for an insurance company and the minimum

amount of insurance coverage sought. It may also require parties to notify changes to the insurance coverage or provide copies of current insurance policies to each other.

K. Remedies for breach of the contract

Types of remedies

138. The parties are free to select remedies within the limits of applicable law. Remedies may include in-kind remedies aimed at providing the aggrieved party with the same or equivalent benefit expected from contract performance (e.g., replacement of the defective hardware), monetary remedies (e.g., service credits) and termination of the contract. The contract could differentiate between types of breaches and specify corresponding remedies.

Suspension or termination of services

139. Suspension or termination of the provision of the cloud computing services is a usual remedy of the provider for the customer's breach of a contract or violation of the **AUP** by the customer's end users. The contract may include safeguards against broad suspension or termination rights. For example, the right of the provider to suspend or terminate the provision of the cloud computing services to the customer may be limited to cases of fundamental breach of the contract by the customer, significant threats to the security or integrity of the provider's system and cases stated in the applicable law. The provider's right to suspend or terminate may also be restricted only to those services that are affected by the breach, where such a possibility exists.

Service credits

140. An often-used mechanism to compensate the customer for non-performance by the provider is the system of service credits. Those credits take the form of a reduced fee for the services to be provided under the contract in the following measured period. A sliding scale may apply, i.e., a percentage of reduction may depend on the extent to which the provider's performance under the contract falls short of the performance parameters identified in **SLA** or other parts of the contract. An overall cap for service credits may also apply. Providers may limit the circumstances in which service credits are given to those, for example, where failures arise from matters under the provider's control or where credits are claimed within a certain period of time. Some providers may also be willing to offer a refund of fees already paid or an enhanced service package in the following measured period (e.g., free information technology consultancy). If a range of options exists, providers' standard terms may stipulate that any remedy for provider non-performance will be at the choice of the provider.

141. Fixing service credits as the sole and exclusive remedy against the provider's non-performance of its contractual commitments may limit the customer's rights to other remedies, including suing for damages or terminating the contract. In addition, service credits in the form of fee reduction or an enhanced service package in the following measured period may be useless if the contract is terminated. Excessive service credits may be unenforceable if they have been considered as an unreasonable approximation of harm at the outset of the contract. Other measures, such as penalties, may provide more appropriate incentives for ensuring contractual compliance.

Formalities to be followed in case of the breach of the contract

142. The contract may include formalities to be followed in cases of breach. For example, the contract could require a party to notify the other party when any terms of the contract are deemed to be violated and to provide a chance to remedy such asserted violation. Time limits for claiming remedies may also be set.

L. Term and termination of the contract

Effective start date of the contract

143. The effective start date of the contract may be different from the signature date, the date of acceptance of the offer or the date of acceptance of configuration and other actions required for the customer to migrate to the cloud. The date when the cloud computing services are made available to the customer by the provider, even if they are not actually used by the customer, may be considered the effective start date of the contract. The date of the first payment by the customer for the cloud computing services, even if they are not yet made available to the customer by the provider, may also be considered the effective start date of the contract. For those reasons and to avoid uncertainties, the parties may indicate in the contract its effective start date.

Duration of the contract

144. The duration of the contract could be short, medium or long. It is common in **standardized commoditized multi-subscriber cloud solutions** to provide for a fixed initial duration (short or medium), with automatic renewals unless terminated by either party. The provider may agree to serve the customer an advance notification of the upcoming expiration of the term of the contract. Various considerations, including risks of being **lock-in** and missing better deals, may impact a decision on renewal.

Earlier termination

145. Contracts usually address reasons for termination other than upon expiration of its fixed term, such as for convenience, breach or other reasons. The contract may provide modalities for earlier termination, including requirements for a sufficiently advance notice, **reversibility** and other end-of-service commitments (see paras. 157–167 below).

Termination of the contract for convenience

146. Providers' standard terms, especially for provision of **standardized commoditized multi-subscriber cloud solutions**, usually reserve the right of the provider to terminate the contract at any time without customer default. The parties may agree to limit the circumstances under which such a right could be exercised and oblige the provider to serve the customer with sufficiently advance notice of termination.

147. The customer's right to terminate the contract for convenience (i.e., without the default of the provider) is especially common in public contracts. The provider may demand payment of early termination fees in such cases. Payment of early termination fees by public entities may however be restricted by law. In contracts of indefinite duration, providers may be more inclined to accept termination by the customer for mere convenience without compensation, but that might also lead to a higher contract price.

Termination for breach

148. Fundamental breach of the contract usually justifies termination of the contract. To avoid ambiguities, the parties may define in the contract events that will be considered by the parties to be a fundamental breach of the contract. The fundamental breach of the contract by the provider may include data loss or misuse, personal data protection violations, recurrent **security incidents** (e.g., more than a certain number of times per any measured period), confidentiality leaks and non-availability of services at certain time points or for a certain period of time. Non-payment by the customer and violation of the **AUP** by the customer or its end users are among the most common reasons for termination of the contract by the provider. The party's right to terminate the contract may be conditional on serving a prior notice, holding good faith consultations and providing a possibility to remedy the situation. The party

may be obliged under the contract to restore contract performance within a certain number of days after remedial action has been taken.

149. The contract may address the provider's end-of-service commitments that would survive the customer's fundamental breach of the contract, including the **reversibility** of customer data and other content (see paras. 157–167 below).

Termination due to unacceptable modifications of the contract

150. Certain modifications to the contract by one party may not be acceptable to the other party and may justify termination of the contract. Those modifications might include modifications to **data localization requirements** or subcontracting terms. The contract may provide for the customer's right to terminate the entire contract if modifications to the contract due to the restructuring of the provider's service portfolio lead to termination or replacement of some services (see paras. 105–124 above and para. 155 below).

Termination in case of insolvency

151. Risks of insolvency may be identified during the risk assessment (see part one, para. 15 (j)) and during the contract, for example, if periodic reporting about the financial condition of the parties is required under the contract. Clauses allowing termination of the contract in the event of insolvency of either party are common. Mandatory provisions of insolvency law may override those clauses.

152. An insolvent customer may need to continue using the cloud computing services while resolving its financial difficulty. The parties may restrict the right to invoke the insolvency as the sole ground for termination of the contract in the absence of, for example, the customer's default in payment under the contract.

153. The parties may specify in the contract, or the law may provide for, mechanisms for the retrieval of customer data in case of the provider's insolvency (e.g., an automatic release of the source code or key escrow allowing access to the customer data and other content). Otherwise, the customer may face difficulties and delays with retrieval of its data and other content from the insolvent provider's cloud infrastructure. Where a mass exit and withdrawal of content occurs due to a crisis of confidence in the provider's financial position, the insolvent provider or an **insolvency representative** may limit the amount of content (data and application code) that can be withdrawn in a given time period or decide that end-of-service commitments should proceed on a "first come, first served" basis.

Termination in case of change of control

154. The change of control may, for example, involve a change in the ownership or the capacity to determine, directly or indirectly, the operating and financial policies of the provider, which may lead to changes in the provider's service portfolio. The change of control may also involve the assignment or novation of the contract, with rights and obligations or only rights under the contract transferred to a third party. As a result, an original party to the contract may change, or certain aspects of the contract, for example payments, may need to be performed to a third party.

155. The applicable law may require termination of the contract if as a result of the change of control, mandatory requirements of law (e.g., **data localization requirements** or prohibition to deal with certain entities under international sanctions regime or because of national security concerns) cannot be fulfilled. Public contracts may, in particular, be affected by statutory restrictions on the change of control. In addition, the parties may agree about termination of the contract in case of change of control, in particular if, as a result of such change, the provider or the contract is taken over by the customer's competitor or if the takeover leads to discontinuation of, or significant changes in, the service portfolio. Requiring an advance notice of an upcoming change of control and its expected impact on the contract is common.

Inactive account clause

156. Customer inactivity for a certain time period specified in the contract may be a ground for unilateral termination of the contract by the provider. The inactive account clause is unusual in business-to-business cloud computing contracts provided for remuneration.

M. End-of-service commitments

157. End-of-service commitments may raise not only contractual but also regulatory issues. The parties may be concerned about achieving a balance between the customer's interest in continuous access to its data and other content, including during the transition period, and the provider's interest in ending any obligation towards the former customer as soon as possible.

158. End-of-service commitments may be the same regardless of the cause of termination of the contract or may be different depending on whether termination is for breach of contract or other reasons. Issues that parties may wish to address in the contract include the following.

Time frame for export

159. The parties may specify in the contract a time frame for export that may need to be sufficiently long to ensure a smooth export by the customer of its data and other content to another system.

Customer access to the content subject to export

160. The contract would specify data and other content subject to export and ways of gaining customer access thereto, including any decryption keys that may be held by the provider or third parties (see part one, para. 28). To facilitate the export of the customer's data with the minimal involvement of the provider, the parties may agree on an escrow arrangement (i.e., involvement of a third party authorized to automatically release to the customer the source code, decryption keys or other elements allowing access to the customer data and other content upon occurrence of certain events, such as termination of the contract (see also para. 153 above)). The contract may also specify export options, including their formats and processes, to the extent possible, recognizing that they may change over time.

Export assistance by the provider

161. The provider may not always agree to be actively involved in assisting the customer with exporting its data to another system, but it may be expected under law to ensure that such export is possible and simple. Where the parties agreed on the provider's involvement in the export of customer data to another system, the contract may specify details, such as the extent, procedure and time period for export assistance. The provider may require separate payment for the provision of export assistance. In such case, the parties may fix the amount of the payment in the contract or agree to refer to the provider's price list at a given time. Alternatively, the parties may agree that such assistance is included in the contract price or that no extra payment will be charged if the contract termination follows the provider's breach of contract.

Data deletion

162. The contract may need to specify rules for **data deletion** from the provider's cloud infrastructure upon export or expiration of the period specified in the contract for export. The data deletion may be done automatically by the provider, for example, upon occurrence of certain events, expiration of time periods that were agreed upon by the parties or as required by law. Alternatively, data may be deleted only upon a specific customer's request and instructions. The parties may agree that the customer will be notified about the upcoming data deletion and will be served with an

attestation, report or statement of data deletion, including data deletion from third parties' systems.

Post-contract retention of data

163. The provider might be required to retain customer data by law, in particular a data protection law, which may also address a time period during which the data must be retained. The parties may agree on the retention of customer data by the provider after the termination of the contract. Some providers may offer a post-contract retention period at additional cost.

164. The parties may include special requirements as regards data that are not or cannot be returned to the customer and whose deletion would not be possible. For example, the contract may specify that all personal information must be de-identified and that the data are to be retained in an encrypted form or in a usable and interoperable format to allow its retrieval when required. The parties may also agree on the responsibilities of the parties for post-contractual retention of the data in the specified format.

Post-contract confidentiality clause

165. The parties may agree on a post-contract confidentiality clause. Confidentiality obligations may survive the contract for a specified number of years after the contract is terminated (e.g., five or seven years), or may continue indefinitely, depending on the nature of the customer data and other content that was placed in the provider's cloud infrastructure.

Post-contract audits

166. Post-contract audits may be agreed by parties or imposed by law. The parties may agree on terms for carrying out such audits, including the time frame and allocation of costs.

Leftover account balance

167. The parties may agree on conditions for the return to the customer of leftover amounts on its account or for the offset of those amounts against any additional payments the customer would need to make to the provider, including for end-of-service activities or to compensate damage.

N. Dispute resolution

Methods of dispute settlement

168. The parties may agree on the method to settle their contractual disputes. Dispute settlement methods include negotiation, mediation, conciliation, online dispute resolution (ODR), arbitration and judicial proceedings. Different types of dispute may justify different dispute resolution procedures. Disputes over financial and technical issues, for example, may be referred to a binding decision by a third party expert (individual or body), while some other types of disputes may be more effectively dealt with through direct negotiations between the parties. In case of smaller claims, ODR-assisted negotiations or mediation may offer fast and cost-effective methods for the parties to reach consensual agreement online. For higher-level claims, cloud sector-specific ODR may offer a competent specialized forum and be helpful for judicial processes. The law of some jurisdictions may prescribe certain alternative dispute resolution mechanisms that the parties would need to exhaust before being able to refer a dispute to a court.

Arbitral proceedings

169. Disputes that are not amicably settled may be referred to arbitral proceedings if the parties opted for it. Not all issues may, however, be referred to arbitration; some

may be reserved by law for adjudication by a court. The parties may therefore wish to verify the arbitrability of their disputes before opting for arbitration. An arbitration clause in a contract would usually refer to a set of arbitration rules to govern arbitral proceedings. A contract can include a standard dispute resolution clause referring to the use of internationally recognized rules for the conduct of dispute resolution proceedings (e.g., the UNCITRAL Arbitration Rules). In the absence of such specification, the arbitral proceedings will normally be governed by the procedural law of the State where the proceedings take place or, if an arbitration institution is chosen by the parties, by the rules of that institution.

Online dispute resolution

170. The parties may opt for an ODR mechanism for some or all categories of disputes arising from their contract subject to limitations imposed by law. The contract may specify the scope of issues subject to ODR and the ODR platform and rules to be used in the proceedings. In some cases, ODR could be embedded in the cloud service package offered by the provider with an opt-out possibility.

171. The ODR process usually consists of: (a) negotiation conducted between the parties via the ODR platform; (b) facilitated settlement, where a neutral is appointed and communicates with the parties to try to achieve a settlement; and (c) a final stage, in which the ODR administrator or a neutral informs the parties of the nature of the final stage, and of its form. The result of ODR may be non-binding on the parties unless the contract or the applicable law states otherwise.

Judicial proceedings

172. If judicial proceedings are to take place, due to the nature of **cloud computing services**, several States might claim jurisdiction. Where possible, parties may agree on a jurisdiction clause under which they are obligated to submit disputes to a specific court (see paras. 175–181 below).

Retention of data

173. During the dispute resolution phase, continued access by the customer to its data, including **metadata** and other **cloud service-derived data,** may be vital, apart from for business continuity, for the customer's participation in dispute resolution proceedings (e.g., to substantiate a claim or counterclaim). The contract may specifically provide that, in case of disputes between the parties, the customer's data will be retained by the provider and the customer will have access to its data for a reasonable period of time, regardless of the nature of the dispute. The parties may also agree on an escrow arrangement (see para. 160 above).

Limitation period for complaints

174. The parties may specify in the contract the limitation period within which claims may be brought. Limitation periods stipulated in the law may be applicable and will override non-compliant terms of the contract.

O. Choice of law and choice of forum clauses

175. Freedom of contract (see para. 34 above) usually allows parties to choose the law that will be applicable to their contract and the jurisdiction or forum where disputes will be considered. The mandatory law (e.g., data protection law) may, however, override the choice of law and the choice of forum clauses made by the contracting parties, depending on the subject of the dispute. In addition, regardless of the choice of law and choice of forum, more than one mandatory law (e.g., data protection law, insolvency law), including from different jurisdictions, may be applicable to the contract.

Considerations involved in choosing the applicable law and forum

176. The choice of law and choice of forum clauses are interconnected. Whether the selected and agreed-upon law will ultimately apply depends on the forum in which the choice-of-law clause is presented to a court or another adjudicating body, e.g., an arbitral tribunal. It is the law of that forum that will determine whether the clause is valid and whether the forum will respect the choice of applicable law made by the parties. Because of the importance of the forum law for the fate of the choice of law clause, a contract with such a clause usually also includes a choice of forum clause.

177. In choosing the forum, the parties usually consider the impact of the chosen or otherwise applicable law and the extent to which a judicial decision made in that forum would be recognized and enforceable in the countries where enforcement would likely be sought. Preserving flexibility in enforcement options may be an important consideration, especially in the cloud computing settings where many factors that parties usually take into account in formulating choice of law and choice of forum clauses may be uncertain, including the location of assets involved in the provision of services and the location of the provider and the customer.

Mandatory law and forum

178. The law and the forum of a particular jurisdiction may be mandatory on various grounds, for example:

(a) The accessibility of the cloud computing services in the territory of a particular State may be sufficient for the application of the data protection law of that State;

(b) The nationality or residence of the affected **data subject** or the contracting parties, in particular the **data controller**, may trigger the application of the law of that **data subject** or the party; and

(c) The law of the place in which the activity originated (the location of the equipment) or to which the activity is directed for the purpose of extracting benefits may trigger the application of the law of that place. The use of a given country top-level domain associated with a particular place, a local language in the website, pricing in local currency and local contact points are among the factors that might be taken into account in making such determination.

Provider or customer home law and forum

179. Contracts for **standardized commoditized multi-subscriber cloud solutions** often specify that they are governed by the law of the provider's principal place of business or place of establishment. They typically grant the courts of that country exclusive jurisdiction over any disputes arising out of the contract. The customer may prefer the law and jurisdiction of its own country. Public institutions would have significant restrictions on their ability to consent to the law and jurisdiction of foreign countries. Providers that operate in multiple jurisdictions may be flexible as regards accepting the choice of the law and forum of the country where the customer is located.

Multiple options

180. The parties may also specify various choice of law and forum options for different aspects of the contract. They may also opt for a defendant's jurisdiction to eliminate the home forum advantage for a plaintiff and thus encourage informal resolution of disputes.

No choice of law or forum

181. The parties may prefer no choice of law or forum clause in their contract, leaving the question open for later discussion if and when needed. That might be considered

the only viable solution in some cases. ODR may also be part of the solution for the questions of jurisdiction and applicable law (see paras. 170–171).

P. Notifications

182. Notification clauses usually address the form, language, recipient and means of notification, as well as when the notification becomes effective (upon delivery, dispatch or acknowledgment of receipt). In the absence of any mandatory legislative provisions, parties may agree upon formalities for notification, which could be uniform or vary depending on the importance and urgency and other considerations. More stringent requirements may be made applicable, for example, in case of suspension or unilateral termination of the contract, as compared to routine notifications. The parties may agree on the deadlines, keeping in mind **reversibility** and business continuity needs. The contract may contain references to any notifications and deadlines imposed by law.

183. The parties may opt for **written** notification to be served at the physical or electronic address of the contact persons specified in the contract. The contract may specify the legal consequences of a failure to notify and of a failure to respond to a notification that requires such a response.

Q. Miscellaneous clauses

184. Parties often group under miscellaneous clauses provisions that do not fall under other parts of the contract. Some of them may contain a standard text appearing in all types of commercial contracts (so called "boilerplate provisions"). Examples include a severability clause allowing the removal of invalid provisions from the contract or a language clause identifying a certain language version of the contract as prevailing in case of conflicts in interpretation of various language versions. Placing contractual clauses among miscellaneous provisions does not diminish their legal significance. Some of them may be tailored by the parties to the specifics of **cloud computing services**.

R. Amendment of the contract

185. Amendments to the contract could be triggered by either party. The contract would address the procedure for introducing amendments and making them effective. The contract may also need to address the consequences of rejection of amendments by either party.

186. In the light of the nature of **cloud computing services**, it might be difficult to differentiate changes that would constitute amendment of the contract from those changes that would not. For example, the customer's use of any options made available from the outset in the contract would not necessarily constitute an amendment of the initial contract, nor would changes in services resulting from routine maintenance and other activities of the provider covered by the contract (see paras. 105–106 above). The addition of features not covered by the originally agreed terms and thus justifying changes in price may, on the other hand, constitute amendment of the contract. Any updates leading to material changes to previously agreed terms and policies may also constitute an amendment of the contract.

187. The extent of permissible modifications to public contracts may be limited by public procurement rules that usually restrict the freedom of parties to renegotiate terms of a contract that were subject to public tendering proceedings.

188. In the light of frequent modifications of the originally agreed terms, each party may wish to independently store the complete set of the originally agreed terms and their modifications.

Glossary

Acceptable use policy (AUP): Part of the cloud computing contract between the provider and the customer that defines the limits of use by the customer and its end users of the cloud computing services covered by the contract.

Audit: The process of examining compliance with contractual and statutory requirements or technical standards. It may cover technical aspects, such as the quality and security of hardware and software; compliance with any applicable industry standards; and the existence of adequate measures, including isolation, to prevent unauthorized access to and use of the system and to assure data integrity. The audit may be internal or external or be done by an independent third party appointed by either the provider, the customer or both. The **service level agreement (SLA)** may contain specific performance parameters related to audit, e.g., that the services provided under the contract are certified at least annually by an independent auditor against a security standard identified in the contract.

Cloud computing services: online services characterized by:

(a) **Broad network access,** meaning that services can be accessed over the network from any place where the network is available (e.g., through the Internet), using a wide variety of devices, such as mobile phones, tablets and laptops;

(b) **Metered delivery**, allowing usage of the resources to be monitored and charged by reference to level of usage (on a **pay-as-you-go** basis);

(c) **Multi-tenancy,** meaning that physical and virtual resources are allocated to multiple users whose data are isolated and inaccessible to one another;

(d) **On-demand self-service**, meaning that services are used by the customer as needed, automatically or with minimal interaction with the provider;

(e) **Elasticity** and **scalability**, meaning the capability for rapidly scaling up or down the consumption of services according to the customer's needs, including large-scale trends in resource usage (e.g., seasonal effects);

(f) **Resource pooling**, meaning that physical or virtual resources can be aggregated by the provider in order to serve one or more customers without their control or knowledge over the processes involved;

(g) A **wide range of services** from the provision and use of simple connectivity and basic computing services (such as storage, emails and office applications) to the provision and use of the whole range of physical information technology infrastructure (such as servers and data centres) and virtual resources needed for the customer to build its own information technology platforms, or deploy, manage and run customer-created or customer-acquired applications or software. Infrastructure as a service **(IaaS),** platform as a service **(PaaS)** or software as a service **(SaaS)** are types of cloud computing services.

Cloud computing service partners (e.g., cloud auditors, cloud service brokers and system integrators): Persons engaged in support of, or auxiliary to, activities of either the provider or the customer or both. Cloud auditors conduct an **audit** of the provision and use of **cloud computing services**. Cloud service brokers or system integrators assist parties with a wide range of issues, e.g., with finding the right cloud solution, negotiating acceptable terms and migrating the customer to the cloud.

Cloud service-derived data: Data under the control of the provider that are derived as a result of the use by the customer of the cloud computing services of that provider. It includes **metadata** and any other log data generated by the provider containing records of who used the services, at what times, which functions and which types of data are involved. It can also include information about authorized users, their identifiers and any configuration, customization and modification.

Data controller: A person that determines the purposes and means of the processing of **personal data**.

Data deletion: A sequence of operations designed to irreversibly erase data, including its backups and metadata, and other content from the cloud computing infrastructure (physical and virtual). In some cases, data deletion may require the destruction of the physical infrastructure (e.g., the servers) on which the data were stored. The **service level agreement (SLA)** may contain a specific performance parameter related to data deletion, e.g., that the provider ensures that the customer's data are effectively, irrevocably and permanently deleted wherever requested by the customer within a certain time period identified in the contract and in compliance with the standard or method identified in the contract.

Data localization requirements: Requirements relating to the location of data and other content or data centres or the provider. They may prohibit certain data (including **metadata** and backups) from residing in or transiting into or out of a certain area or jurisdictions or require that prior approval be obtained from a competent State body for that. They are often found in data protection law and regulations, which may in particular prohibit **personal data** from residing in or transiting into jurisdictions that do not adhere to certain standards of personal data protection.

Data processor: A person that processes the data on behalf of the **data controller**.

Data subject: A natural person who can be identified, directly or indirectly, by data, including by reference to such identifiers as name, an identification number, location and any factors specific to the physical, genetic, mental, economic, cultural or social identity of the person. In a number of jurisdictions, data subjects enjoy under data protection or data privacy regulations certain rights with respect to the data that can identify them. Those regulations may trigger the inclusion in the **service level agreement (SLA)** of data protection-specific performance parameters, such as that the services provided under the contract are certified at least annually by an independent auditor against the data protection/privacy standard identified in the contract. (See also **data subject's rights** and **personal data**)

Data subjects' rights: Rights associated with **data subjects' personal data**. **Data subjects** under law may enjoy the right to be informed about all significant facts related to their personal data, including data location, use by third parties and data leaks or other data breaches. They may also have the right to access their personal data at any time, the right to erasure of their personal data (pursuant to the right to be forgotten), the right to restrict **processing** of their personal data and the right to **portability** of their personal data.

Deployment models: The various ways in which cloud computing services are organized, based on the control and sharing of physical or virtual resources:

(a) **Public cloud,** where **cloud computing services** are potentially available to any interested customer and resources are controlled by the provider;

(b) **Community cloud,** where **cloud computing services** exclusively support a specific group of related customers with shared requirements and resources are controlled by at least one member of that group;

(c) **Private cloud,** where **cloud computing services** are used exclusively by a single customer and resources are controlled by that customer;

(d) **Hybrid cloud,** where at least two different cloud deployment models are used.

Downtime or **outages**: The time when the cloud computing services are not available to the customer. That time is excluded from the calculation of **uptime** or availability. Time for maintenance and upgrades is usually included in downtime. It may be defined in the **service level agreement (SLA)** as a number of permissible outages of a specified time duration for a given period, e.g., not more than one outage of one hour per day and not between 8:00 and 17:00.

First response time: The time between when the customer reports an incident and the provider's initial response to it.

Follow-the-sun: A model in which the workload is distributed among different geographical locations to more efficiently balance resources and demand. The purpose of the model may be to provide round-the-clock services and to minimize the average distance between servers and end users in an effort to reduce **latency** and maximize the speed with which data can be transmitted from one device to another (data transfer rate (DTR) or throughput).

Infrastructure as a service (IaaS): Types of **cloud computing services** with which the customer can obtain and use processing, storage or networking resources. The customer does not manage or control the underlying physical or virtual resources, but does have control over operating systems, storage and deployed applications that use the physical or virtual resources. The customer may also have limited ability to control certain networking components (e.g., host firewalls).

Insolvency representative: A person or body authorized in insolvency proceedings to administer the reorganization or the liquidation of the assets of the insolvent debtor that are subject to the insolvency proceedings.

Interoperability: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

Intellectual property (IP) licences: Agreements between an IP rights owner (the licensor) and a person authorized to use those IP rights (the licensee). They usually impose restrictions and obligations on the extent and manner in which the licensee or third parties may use the licenced property. For example, software and visual content (designs, layouts and images) may be licensed for specific use, not allowing copying, modification or enhancement, and be restricted to a certain medium. The licences may be limited to a particular market (e.g., national or (sub)regional), a number of users or a number of devices, or may be time-bound. Sub-licensing may not be permitted. The licensor may require reference to be made to the IP rights owner each time the IP rights are used.

Latency: The delay between a user's request and a provider's response to it. It affects how usable the **cloud computing services** actually are. In the **service level agreement (SLA)**, the latency is usually expressed in milliseconds.

Layered cloud computing services: Where the provider is not the owner of all or any computing resources that it uses for the provision of the cloud computing services to its customers but is itself the customer of all or some **cloud computing services**. For example, the provider of **platform as a service (PaaS)** or **software as a service (SaaS)** types of service may use storage and server infrastructure (data centres, data servers) owned or provided by another entity. As a result, one or more sub-providers may be involved in providing the cloud computing services to the customer. The customer may not know which layers are involved in the provision of services at a given time, which makes identification and management of risks difficult. Layered cloud computing services are common in **SaaS** in particular.

Lock-in: Where the customer is dependent on a single provider because the costs of switching to another provider are substantial. Costs in this context are to be understood in the broadest sense as encompassing not only monetary expenses but also effort, time and relational aspects.

Metadata: Basic information about data (such as author, when the data were created, when they were modified and file size). It makes finding and using the data easier and may be required to ensure the authenticity of the record. It can be generated by the customer or the provider.

Performance parameters: Quantitative parameters (numerical targets or metrics or a performance range) or qualitative parameters (service quality assurances). They may refer to conformity with applicable standards, including the date of expiry of any conformity certification (e.g., that the provider has implemented a key management policy in compliance with the international standard identified in the contract). To be meaningful, the parameters should allow the customer to measure performance that is

important to the customer in an easy and auditable way. They could be different depending on the risks involved and business needs (e.g., the criticality of certain data, services or applications and the corresponding priority for recovery). For example, a non-mission critical system that is designed to use the cloud for archival purposes will not need the same **uptime** or other **service level agreement (SLA)** terms as mission critical or real-time operations.

Persistency of data storage: The probability that data stored in the cloud will not be lost during the contract period. It can be expressed in the contract as a measurable target against which the customer will measure steps taken by the provider to ensure persistency of data storage (e.g., intact data/intact data + lost data during an identified period of time (e.g., a calendar month)). The type of data (e.g., files, databases, codes, applications) and the unit of measurement (the number of files, bit length) would need to be defined in that formula.

Personal data: Sensitive and non-sensitive data that can be used to identify the natural person to whom such data relate. The definition of personal data in some jurisdictions may encompass any data or information directly or indirectly linked or relating to an identified or identifiable individual (see the **data subject**).

Personal data processing: The collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

Platform as a service (PaaS): Types of **cloud computing services** with which the customer can deploy, manage and run in the cloud customer-created or customer-acquired applications using one or more existing programming languages and execution environments supported by the provider.

Portability: The ability to easily transfer data, applications and other content from one system to another (i.e., at low cost, with minimal disruption and without being required to re-enter data, re-engineer processes or re-program applications). This might be achieved if it is possible to retrieve the data in the format that is accepted in another system or with a simple and straightforward transformation using commonly available tools. The **service level agreement (SLA)** may contain performance parameters related to portability, e.g., the customer data is retrievable by the customer via a single download link or documented application programming interfaces (API); or the data format is structured and documented in a sufficient manner to allow the customer to re-use it or to restructure it into a different data format if desired.

Recovery point objectives (RPOs): The maximum time period prior to an unplanned interruption of services during which changes to data may be lost as a consequence of recovery. If RPO is specified in the contract as two hours before the interruption of services, that would mean that all data would be accessible after recovery in the form those data existed two hours before the interruption occurred.

Recovery time objectives (RTO): The time period within which all cloud computing services and data must be recovered following an unplanned interruption.

Reversibility: The process for the customer to retrieve its data, applications and other related content from the cloud and for the provider to delete the customer data and other related content after an agreed period.

Sector-specific regulations: Financial, health, public sector or other specific sector or profession regulations (e.g., attorney-client privilege, medical professional secrecy) and rules for handling classified information (broadly understood as information to which access is restricted by law or regulation to particular classes of persons).

Security incident: An event that indicates that the system or data have been compromised or that measures put in place to protect them have failed. A security incident disrupts normal operations. Examples of security incidents include attempts from unauthorized sources to access systems or data, unplanned disruption to a

service or denial of a service, unauthorized processing or storage of data and unauthorized changes to system infrastructure.

Service level agreement (SLA): Part of the cloud computing contract between the provider and the customer that identifies the cloud computing services covered by the contract and the level of service expected or to be achieved under the contract (see the **performance parameters**).

Software as a service (SaaS): Types of **cloud computing services** with which the customer can use the provider's applications in the cloud.

Standardized commoditized multi-subscriber cloud solutions: **Cloud computing services** provided to an unlimited number of customers as a mass product or commodity on non-negotiable standard terms of the provider. Broad disclaimers and waivers of the provider's liability are common in this type of solution. The customer may be in a position to compare different providers and their contracts and select among those available on the market the most suitable for its needs, but not to negotiate a contract.

Uptime: The time when the cloud computing services are accessible and usable. It may be expressed as the amount or percentage, a detailed formula or specific dates or days and time when availability of the service of a particular application is critical.

Written or **in writing**: Information accessible so as to be usable for subsequent reference. It encompasses information on paper and in an electronic communication. "Accessible" means that information in the form of computer data should be readable and interpretable and that the software that might be necessary to render such information readable should be retained. "Usable" covers both human use and computer processing.